



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/682,256	08/10/2001	Ta-Kuang Yang	MSV001	1851

7590 11/18/2004
NAIPO (North America International Patent Office)
P.O. Box 506
Merrifield, VA 22116

EXAMINER

NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/682,256

Applicant(s)

YANG, TA-KUANG

Examiner

Tremayne M. Norris

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: In paragraph 21, the words "is" and "a" need to be separated.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-8,10-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Sasaki (US pat 6,351,536).

Regarding claim 1, Sasaki teaches a method to prevent illegal copying of an electronic document in a computer system, the computer system comprising a server for connecting to a plurality of terminals via a network, each terminal having a terminal

identification code for identifying the terminal, each terminal capable of requesting an electronic document from the server via the network, the server capable of encrypting original plaintext of the electronic document to a corresponding ciphertext, the ciphertext capable of being transmitted to the terminal via the network and being decrypted to the original plaintext, the method comprising a registration process and a document request process, the registration process comprising:

- installing a reading application program in a terminal, the reading application program comprising a first secret key (col.7 lines 36-41);

- utilizing the reading application program to register the terminal with the server (col.3 lines 28-39; col.10 lines 5-9; col.10 lines 30-34);

- encrypting (col.2 lines 4-7) and transmitting to the terminal a user identification code and a second secret key, the user identification code and the second secret key being generated by the server (col.7 lines 8-35; col.7 lines 54-59); and

- generating a terminal encryption file by encrypting the user identification code, the second secret key, and the terminal identification code, the terminal encryption file being stored in the terminal (col.17 lines 18-23; col.17 lines 48-51; col.20 lines 55-59);

- the document request process comprising:

- a terminal requesting the server for an electronic document, the server using the second secret key to encrypt plaintext of the electronic document to corresponding ciphertext, the ciphertext being transmitted to the terminal via the network (col.7 lines 30-35);

using the first secret key to decrypt the terminal encryption file to retrieve the second secret key and the terminal identification code (col.7 line 66 thru col.8 line 6); and

utilizing the retrieved second secret key to decrypt the received ciphertext if a run-time terminal identification code corresponds to the terminal identification code retrieved from the terminal encryption file, otherwise terminating further decryption to prevent illegal copying of the electronic document by unregistered terminals (col.3 lines 28-39).

Regarding claim 2, Sasaki teaches the terminal further comprises a central processing unit (CPU), a hard-disk, and a network card, and the terminal identification code is selected from one of an identification code from the CPU, the hard-disk, or the network card (fig.2; col.5 line 57 thru col.6 line 6; col.9 lines 46-51).

Regarding claim 3, Sasaki teaches the server comprises a user database for recording a plurality of user identification codes of registered users, and terminal identification codes (col.7 lines 12-29; col.9 lines 46-51).

Regarding claim 4, Sasaki teaches the server comprises a secret key generating module for generating a second secret key for each user registered in the user database (col.7 lines 8-29).

Regarding claim 5, Sasaki teaches the server comprises a key database for recording the user identification codes of the registered users, and the associated second secret keys (col.7 lines 8-29).

Regarding claim 6, Sasaki teaches the server comprises an encryption module for encrypting and transmitting to the terminal the second secret key and the user identification code (col.2 lines 4-7; col.7 lines 30-35; col.7 lines 54-59).

Regarding claim 7, Sasaki teaches the server comprises an electronic document database for storing associated plaintexts of a plurality of electronic documents, and a control center for controlling operations of the server (fig.2 element 13; col.6 line 66 thru col.7 line 7).

Regarding claim 8, Sasaki teaches when the server receives a request for the electronic document by the terminal, the control center locates the associated plaintext of the electronic document, and the encryption module encrypts the plaintext of the electronic document with the second secret key to form the corresponding ciphertext (col.7 lines 30-32).

Regarding claim 10, Sasaki teaches the server comprises a public software module for storing the reading application program to be downloaded to the terminals by users (col.8 lines 27-32).

System claims 11-16 are substantially equivalent to method claims 1-3,5,7, and 8 respectively, therefore claims 11-16 are rejected for the same reasons.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 9 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki, and further in view of Schneier.

Regarding claim 9, Sasaki teaches the method of claim 1, but does not teach the first secret key and the second secret key are both 128-bit encryption keys. Schneier teaches 128-bit encryption keys (p.154 last paragraph thru page 155 first paragraph). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Sasaki's encryption network system with Schneier's teaching of 128-bit encryption keys in order to prevent brute-force attacks that try recover session keys (Schneier p.154 last paragraph thru page 155 first paragraph).

Claim 17 is a system claim that is substantially equivalent to method claim 9, therefore claim 17 is rejected for the same reasons.

Conclusion

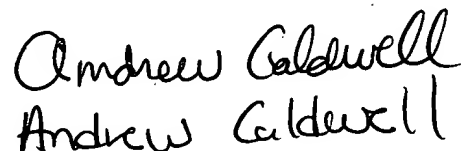
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (571) 272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

November 12, 2004



Andrew Caldwell
Andrew Caldwell